# ON A THEOREM OF HIGHER RECIPROCITY*

BY LEONARD CARLITZ

1. *Introduction.* Let $\mathfrak{D}$ denote the totality of polynomials in an indeterminate, $x$, with coefficients in a fixed Galois field of order $p^n$. Let $P$ be a primary irreducible element of $\mathfrak{D}$; then, if $A$ is any polynomial in $\mathfrak{D}$ not divisible by $P$,

$$A^{p^{n\nu}-1} \equiv 1 \pmod{P},$$

where $\nu$ is the degree of $P$. Evidently then

$$A^{(p^{n\nu}-1)/(p^n-1)}$$

is congruent (mod $P$) to a quantity in the $GF(p^n)$, that is, to a polynomial of degree zero. We define $(A/P)$, the residue character of index $p^n-1$, as that element of $GF(p^n)$ for which

$$\left(\frac{A}{P}\right) \equiv A^{(p^{n\nu}-1)/(p^n-1)} \pmod{P}.$$

We have then the following theorem of reciprocity, proved in a recent paper.†

*If $P$ and $Q$ are primary irreducible polynomials in $\mathfrak{D}$ of degree $\nu$ and $\rho$ respectively, then*

$$\left(\frac{P}{Q}\right) = (-1)^{\rho\nu}\left(\frac{Q}{P}\right). \tag{1}$$

The purpose of this note is to give a simple new proof of this theorem along the lines of Zeller's well known proof of the ordinary quadratic reciprocity theorem.‡

2. *Analog of Gauss' Lemma.* If $A$ is in $\mathfrak{D}$, then sgn $A$ denotes the coefficient of the highest power of $x$ which occurs in $A$; if sgn $A=1$, $A$ is *primary*. Let $\mathfrak{R}(A/B)$ denote the remainder in the division of $A$ by $B$. Then the analog in question is furnished by the following theorem.

---

* Presented to the Society, December 27, 1932.

† American Journal of Mathematics, vol. 54 (1932), pp. 39–50.

‡ Monatsbericht der Berliner Akademie, December, 1872.

LEMMA. *Let $A$ and $P$ be in $\mathfrak{D}$, $P$ primary irreducible, and not a divisor of $A$; then*

$$\left(\frac{A}{P}\right) = \prod_H \operatorname{sgn} \mathfrak{R}\left(\frac{HA}{P}\right), \tag{2}$$

*the product extending over all primary $H$ of degree less than the degree of $P$.*

A detailed proof of this lemma is scarcely necessary, but we remark for a later purpose that the proof depends on the fact that the set of polynomials

$$\left\{ \mathfrak{R}\left(\frac{HA}{P}\right) \Big/ \operatorname{sgn} \mathfrak{R}\left(\frac{HA}{P}\right) \right\}$$

is identical (except for order) with the set $\{H\}$, where $H$ runs through the primary polynomials of degree less than the degree of $P$.

3. *Proof of the Theorem.* Let $\{bM\}$ denote the set of those polynomials in the set

$$\left\{ \mathfrak{R}\left(\frac{HQ}{P}\right) \right\}, \qquad (\deg H < \nu, \operatorname{sgn} H = 1),$$

with signum equal to $b$, a fixed quantity in $GF(p^n)$. We write $S_b = \{M\}$; evidently the polynomials $M$ are primary. Similarly we put $S_b' = \{N\}$, where $\{bN\}$ denotes the set of those polynomials in the set

$$\left\{ \mathfrak{R}\left(\frac{KP}{Q}\right) \right\}, \qquad (\deg K < \rho, \operatorname{sgn} K = 1),$$

with signum equal to $b$.

We assume, as we may without any loss in generality, that $\rho \geqq \nu$. We put

$$S_b' = U_b + V_b, \tag{3}$$

where

$$U_b = \{M \text{ in } S_b'; \deg M < \nu\},$$
$$V_b = \{M \text{ in } S_b'; \deg M \geqq \nu\}.$$

Then we begin by proving

$$U_b = S_{-b}. \tag{4}$$

Indeed, let $M$ be any polynomial in $S_b$, that is, let

$$HQ \equiv bM \pmod{P},$$

where $\deg H < \nu$, $\operatorname{sgn} H = 1$. Evidently there exists a primary $K$ of degree $< \rho$ such that

$$HQ = bM + KP.$$

But this equality may be written in the form

$$KP \equiv -bM \pmod{Q},$$

and since $\deg M < \nu$, it follows at once that $M$ is in $U_{-b}$.

Conversely assume an $M$ in $U_b$. Then there exists a primary $K$ of degree $< \rho$, such that

$$KP \equiv bM \pmod{Q};$$

since $\deg M < \nu$, we infer the existence of a primary (in particular, non-zero) $H$ of degree $< \nu$, such that

$$KP = bM + HQ.$$

Then it follows as above that $M$ is in $S_{-b}$. We have therefore set up a (1, 1) correspondence between the elements of $U_b$ and $S_{-b}$, thus proving equation (4).

Let us write $\mu(W)$ for the number of elements in a (finite) set $W$. Then, by Gauss' Lemma and equation (3),

$$\left(\frac{P}{Q}\right) = \prod_{b \neq 0} b^{\mu(U_b) + \mu(V_b)}, \tag{5}$$

the product in the right member extending over all $b$ in $GF(p^n)$ different from zero. By equation (4), the right side of (5) may be written in the form

$$\prod_b b^{\mu(S_{-b}) + \mu(V_b)}.$$

Now

$$\prod_b b^{\mu(S_{-b})} = \prod_b (-b)^{\mu(S_b)} = \prod_b (-1)^{\mu(S_b)} \cdot \prod_b b^{\mu(S_b)}; \tag{6}$$

but (by the remark in §2)

$$\sum_b \mu(S_b) = \frac{p^{n\nu} - 1}{p^n - 1} \equiv \nu \pmod{2}, \tag{7}$$

and by Gauss' Lemma

$$\prod_b b^{\mu(S_b)} = \left(\frac{Q}{P}\right); \tag{8}$$

we have therefore, by equations (5), $\cdots$, (8),

$$\left(\frac{P}{Q}\right) = (-1)^\nu \left(\frac{Q}{P}\right) \prod_b b^{\mu(V_b)}. \tag{9}$$

It remains to calculate $\mu(V_b)$; evidently we may ignore the case $b=1$.

Let $M$ be in $V_b$, so that for some primary $K$ of degree $<\rho$,

$$KP \equiv bM \pmod{Q}. \tag{10}$$

Since the degree of $M$ is not less than the degree of $P$, we may put

$$M = AP + cB, \quad \deg B < \nu,$$

where $A$ and $B$ are primary, and $c$ is in $GF(p^n)$. Then (10) becomes

$$(K - bA)P \equiv cB \pmod{Q}. \tag{11}$$

But

$$\deg A = \deg M - \deg P < \rho - \nu,$$

and since we are assuming $b \neq 1$, we have necessarily

$$\deg K \geqq \rho - \nu.$$

Therefore $K - bA$ is primary and

$$\rho - \nu \leqq \deg (K - bA) < \rho,$$

and finally $B$ is in $U_c$.

Conversely, let us begin with a $B$ in $U_c$:

$$KP \equiv cB \pmod{Q}, \quad \deg B < \nu. \tag{12}$$

Then, if $m$ is an integer such that

$$\nu \leqq m < \rho, \tag{13}$$

and $A$ is a primary polynomial of degree $m-\nu$, we have

$$(K + bA)P \equiv bAP + cB \pmod{Q};$$

and if we put

$$bAP + cB = bM,$$

it is evident that $M$ is in $V_b$. Indeed

$$\deg (K + bA) = \deg K,$$
$$\operatorname{sgn} (K + bA) = \operatorname{sgn} K = 1;$$
$$\deg M = \deg AP = m,$$
$$\operatorname{sgn} M = b^{-1} \operatorname{sgn} (bAP + cB) = 1.$$

To sum up, we have proved that, for fixed $b \neq 1$,

(i) to each element of $V_b$ corresponds a single element of some $U_c$;

(ii) to each element of $U_c$, $c$ fixed, corresponds $p^{n(m-\nu)}$ elements of $V_b$ of degree $m$, where $m$ is a fixed integer satisfying the inequalities (13).

Evidently (ii) implies that the total number of elements of $V_b$ corresponding to a fixed element of $U_c$ is precisely

$$\sum_{m=\nu}^{\rho-1} p^{n(m-\nu)} = \frac{p^{n(\rho-\nu)} - 1}{p^n - 1}.$$

We have therefore that the number of elements in $V_b$ is

$$\mu(V_b) = \frac{p^{n(\rho-\nu)} - 1}{p^n - 1} \, \frac{p^{n\nu} - 1}{p^n - 1}, \tag{14}$$

as follows at once from equations (4) and (7).

Returning to equation (9), we have, since the right member of (14) is independent of $b$,

$$\prod_b b^{\mu(V_b)} = \left(\prod_b b\right)^{\epsilon}, \tag{15}$$

$\epsilon$ denoting the right side of (14).

Now, by the generalization of Wilson's Theorem for a Galois field,

$$\prod_b b = -1;$$

on the other hand

$$\epsilon \equiv (\rho - \nu)\nu \equiv \rho\nu + \nu \pmod 2;$$

therefore, by (9) and (15),

$$\left(\frac{P}{Q}\right) = (-1)^{\rho\nu}\left(\frac{Q}{P}\right).$$

This completes the proof of our theorem of higher reciprocity.

4. *Remarks.* It should be clear that the case $p=2$ is by no means ruled out in the proof just given. Since in the $GF(2^n)$, $+1$ and $-1$ are the same, the theorem in this case assumes the simpler form

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right), \qquad (p = 2),$$

$(P/Q)$ being the residue character of index $2^n-1$.

Secondly, if in the notation of §3, we put

$$W_b = \{M \text{ in } S_b' \, ; \deg M \leqq \nu\}$$

and

$$X_b = \{M \text{ in } S_b' \, ; \deg M > \nu\},$$

then it is easy to show that

$$\prod_b b^{\mu(X_b)} = (-1)^{\rho\nu},$$

or, what amounts to the same thing,

$$\prod_b b^{\mu(W_b)} = \left(\frac{Q}{P}\right).$$

Duke University